PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-156892
(43)Date of publication of application : 06.06.2000

(51)Int.Cl. H04Q 7/38
H04M 1/68
H04Q 7/34
// H04L 9/38

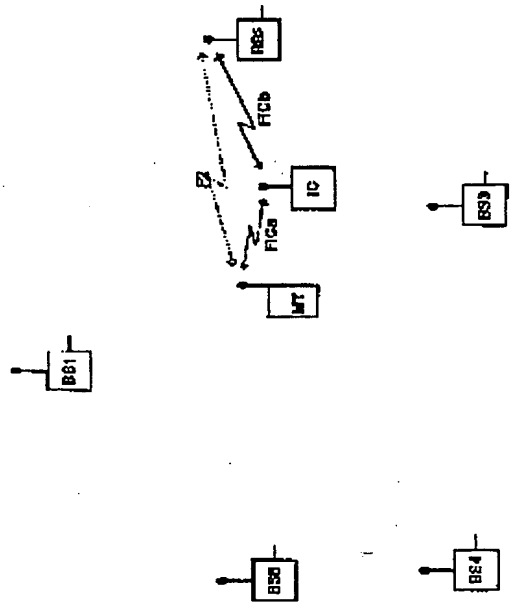
(21)Application number : 11-293346
(22)Date of filing : 15.10.1999

(71)Applicant : ALCATEL
(72)Inventor : WILHELM MICHAEL

(30)Priority
Priority number : 98 19848915 Priority date : 23.10.1998 Priority country : DE

(54) IMPROVEMENT IN SECRECY PROTECTION OF MOBILE TELEPHONE FROM WIRE TAPPING

(57)Abstract:
PROBLEM TO BE SOLVED: To realize a method for detecting a wire tapping device between a mobile telephone and a base station and capable of receiving a call from the mobile telephone as a base station and transferring the received call to the base station as a mobile telephone.
SOLUTION: The data of base stations BS1 to BS5 used by a mobile telephone(MT) are stored in the MT. When new connection to the base station BS2 is established, data newly settled during the establishment of the connection are compared with data expected to the base station BS2 considering the stored data. When both the data are different from each other, an error signal is generated in the MT. The error signal starts disconnection from the base station BS2 or triggers a warning message to a user. Thus the secrecy protection of a GSM mobile station from wire tapping can be improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－156892
（P2000－156892A）
(43)公開日　平成12年６月６日(2000.6.6)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｑ　7/38		Ｈ０４Ｑ	7/04	Ｆ
Ｈ０４Ｍ　1/68		Ｈ０４Ｍ	1/68	
Ｈ０４Ｑ　7/34		Ｈ０４Ｂ	7/26	１０９Ｌ
// Ｈ０４Ｌ　9/38				１０９Ｒ
		Ｈ０４Ｑ	7/04	Ｂ

審査請求　未請求　請求項の数10　ＯＬ　外国語出願　（全 19 頁）　最終頁に続く

(21)出願番号　特願平11－293346

(22)出願日　平成11年10月15日(1999.10.15)

(31)優先権主張番号　１９８４８９１５．３

(32)優先日　平成10年10月23日(1998.10.23)

(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　391030332
アルカテル
フランス国、75008　パリ、リュ・ラ・ボエティ　54

(72)発明者　ミヒヤエル・ピルヘルム
ドイツ国、71665・フアイヒンゲン／エー・エン・ツエツトークライングラツトパツハ、ピルヘルムシユトラーセ・16

(74)代理人　100062007
弁理士　川口　義雄　（外２名）

(54)【発明の名称】　移動電話の盗聴に対する機密保護の改善

(57)【要約】
【課題】　移動電話（ＭＴ）と基地局（ＢＳ２）の間に置かれ、基地局とされる局として移動電話（ＭＴ）からの呼を受け取り、次にそれを、移動電話とされる電話として基地局（ＢＳ２）へ転送する盗聴装置（ＩＣ）を探知する方法を提供すること。
【解決手段】　移動電話（ＭＴ）によって使用された基地局（ＢＳ１、．．．．、ＢＳ５）のデータをその移動電話（ＭＴ）内に記憶させる。基地局（ＢＳ２）への新たな接続が確立されたときに、その接続確立中に新たに確定されたデータが、記憶されているデータを考慮してその基地局（ＢＳ２）に予期されるデータと比較される。データが異なる場合に移動電話（ＭＴ）内でエラー信号が発生する。このエラー信号が、この基地局（ＢＳ２）への接続の解除を開始するか、あるいはユーザへの警告メッセージをトリガする。このようにして、例えば、ＧＳＭ移動ステーションの盗聴に対する機密保護が改善される。

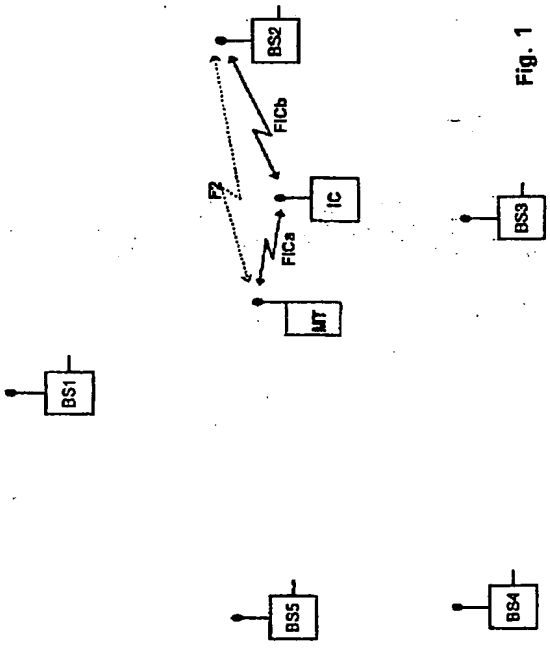


Fig. 1

【特許請求の範囲】
【請求項１】　移動電話（ＭＴ）と基地局（ＢＳ２）の間に置かれ、基地局とされる局（ＢＳ'）として移動電話（ＭＴ）からの呼を受け取り、次にそれを、移動電話とされる電話（ＭＴ'）として基地局（ＢＳ２）へ転送する盗聴装置（ＩＣ）を探知する方法であって、
移動電話（ＭＴ）によって使用された基地局（ＢＳ１、．．．、ＢＳ５）のデータがその移動電話（ＭＴ）内に記憶され、基地局（ＢＳ２）への新たな接続が確立されたときに、その接続確立中に新たに確定されたデータが、記憶されているデータを考慮して前記基地局（ＢＳ２）に予期されるデータと比較され、そのデータが異なる場合に移動電話（ＭＴ）内でエラー信号が発生することを特徴とする方法。
【請求項２】　エラー信号が前記基地局（ＢＳ２）への接続の解除を開始することを特徴とする請求項１に記載の方法。
【請求項３】　エラー信号がユーザへの警告メッセージをトリガすることを特徴とする請求項１に記載の方法。
【請求項４】　データとして、伝搬遅延、および／または基地局（ＢＳ２）が移動電話（ＭＴ）に割り当てた送信電力、および／または基地局（ＢＳ２）が指定した暗号化モードが使用されることを特徴とする請求項１に記載の方法。
【請求項５】　データが、無線セルの識別情報および／または基地局の識別情報を含むことを特徴とする請求項１に記載の方法。
【請求項６】　データが、移動電話（ＭＴ）と基地局（ＢＳ２）の間の距離に応じて記憶されることを特徴とする請求項１に記載の方法。
【請求項７】　データが、互いにある距離だけ隔てられた少なくとも３つの基地局にそれぞれ関係するいくつかのグループに記憶されることを特徴とする請求項６に記載の方法。
【請求項８】　移動電話（ＭＴ）がデータ間の確定された差異を地理的位置に関する情報と共にセンターに伝達することを特徴とする請求項１に記載の方法。
【請求項９】　請求項１から８のいずれか一項に記載の方法を実行するプログラムが記憶されているコンピュータ読取り可能記憶媒体。
【請求項１０】　請求項１から８のいずれか一項に記載の方法を実行するプロセッサ制御式回路を備えるか、または請求項９に記載のコンピュータ読取り可能記憶媒体を備えた移動電話（ＭＴ）。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、移動電話と基地局の間に置かれ、基地局とされる局として移動電話からの呼を受け取り、次にそれを移動電話とされる電話として基地局へ転送する盗聴装置を探知する方法、ならびにその方法を実行するプログラムモジュールおよびそのようなプログラムモジュールを備えた移動電話に関する。
【０００２】
【従来の技術】ＧＳＭ（移動通信グローバルシステム）から知られているように、デジタル移動電話での通話は、移動電話と基地局の間のすべての無線通信が暗号化されるので、盗聴から保護されると考えられている。ジャーナルｃ't　１９９８、Ｎｏ．５、第９２頁に掲載の"Ｈａｎｄｙｓ　ａｂｈｏｒｓｉｃｈｅｒ？"と題する記事ならびにジャーナルＦＯＣＵＳ、３８／１９９７、第２２０／２２１頁に掲載の"Ａｕｓ　ｄｅｒ　Ｌｕｆｔ　ｇｅｇｒｉｆｆｅｎ"と題する記事には、ＩＭＳＩキャッチャー（ＩＭＳＩ＝国際移動加入者識別）と呼ばれる盗聴装置は移動電話の呼を傍受することは結局のところ可能であると記述されている。
【０００３】
【発明が解決しようとする課題】これらの盗聴装置は移動電話と相対して移動無線ネットワークの基地局のように動作する。盗聴装置がその近辺で最強の送信機である場合には、移動電話は次の呼の発信中それを基地局として使用する。各基地局は、呼を確立する間に無線通信の暗号化方法を決定することができるので、盗聴装置は非暗号化モードを選択するであろう。盗聴装置は、本物の基地局ではないので、移動電話とされる電話として隣接の基地局にログオンし、傍受した呼を、あたかも移動電話から発信された呼であるかのように、単に転送する。
【０００４】ＥＰ０８２２７２６Ａ２から、固定電話とその接続先基地局との間の伝搬遅延を基地局で記憶することによって、無線通信ネットワークの機密保護が改善されることがわかっている。次の呼をしようとする間に計測された伝搬遅延が、記憶されている伝搬遅延と異なる場合には、その電話は基地局へのアクセスを拒否される。
【０００５】本発明の目的は、上記の盗聴装置の介在を探知する方法、その方法を実行するプログラムモジュール、およびそのようなプログラムモジュールを備えた移動電話を提供することである。
【０００６】
【課題を解決するための手段】この目的を達成するために、本発明は、移動電話によって使用される基地局の特性データをその移動電話内に記憶させ、新たに基地局への接続が確立されたときにその接続確立中に新たに確定されたデータが、記憶されているデータを考慮して前記基地局に予期されるデータと比較され、そのデータが異なる場合にその移動電話内でエラー信号が発生することを特徴とする最初に言及した種類の方法を提供する。
【０００７】新たに確定されたデータが、盗聴装置が介在する場合のように、記憶されてあるデータと明らかに異なる場合には、エラー信号が視覚的な、可聴な、あるいは機械的な警告メッセージを移動電話からユーザに発

生するか、あるいはその移動電話が他の基地局に切り換わる。この手段が、例えば、ＧＳＭ移動局の盗聴に対する機密保護を改善する。警告メッセージを、例えばさらに別の調査のためにセンターへ送信することもでき、場合により他の移動加入者からの別の警告メッセージを使用して盗聴装置の正確な地上位置を確定することができる。

【０００８】その特性データとしては、伝搬遅延、あるいは基地局が移動電話に割り当てた送信電力が好ましい。さらに基地局が望む非暗号化モードをエラー信号のトリガとして使用することができる。別の特性データとしては、例えば、無線セルまたは基地局の識別情報（identity）、問合わせに対する応答時間、基地局までの地上距離、移動電話の呼についての統計データなどでもよい。

【０００９】これらの特性データは、中間距離での特性データを補間することができるように、移動電話と基地局の間の距離に応じて記憶されるのが好ましい。

【００１０】特性データを、ある距離だけ隔てられた少なくとも３つの基地局にそれぞれ関係するいくつかのグループに記憶する場合には、それぞれの基地局への伝搬遅延などの相互依存データが得られる。

【００１１】移動電話が、データ間の確定された差異を地上位置に関する情報と共に基地局を介してセンターに伝達する場合には、後者は、他の移動電話から受信した別のメッセージを使用して、盗聴装置の正確な地上位置を確定することができる。

【００１２】別の様態によれば、本発明は、さらに、すでに説明した方法を実行するためのハードウェアとソフトウェアのモジュールに関する。

【００１３】

【発明の実施の形態】本発明の別の利点は、以下の説明および添付の図面から明らかである。本発明によれば、上記の特徴および下記の特徴を単独であるいは任意の組合せで使用することができる。本発明の具体的な実施形態について説明するが、説明は例示的なものにすぎず、本発明の範囲を限定するものではないことを理解すべきである。

【００１４】図１は、いくつかの基地局ＢＳ１からＢＳ５までと、盗聴装置ＩＣ（「ＩＭＳＩキャッチャー」）を含む移動無線ネットワークを示す。この盗聴装置ＩＣは、移動局あるいは移動電話ＭＴと相対して移動無線ネットワークの基地局のように動作する。ここに示す実施形態では、移動電話ＭＴは、盗聴装置ＩＣが存在しないかあるいは活動していない場合には、無線リンクＦ２上の呼の確立をするため最強の局として基地局ＢＳ２を選択すると仮定している。しかし、移動電話ＭＴの近辺では、盗聴装置ＩＣが最強の送信機であるので、移動電話ＭＴは、次の呼の発信中、それを、基地局ＢＳ’（図２）と仮定して使用する。このようにして、盗聴装置ＩＣへのリンクＦＩＣａが確立される。各基地局は、接続確立の間に、無線通信の暗号化方式を決定することができるので、盗聴装置ＩＣは非暗号化モードを選択するであろう。そして通話が、盗聴装置ＩＣ内の装置ＲＥＣを介して、聴取され、または録音される。リンクＦＩＣｂを介して、盗聴装置ＩＣが、移動電話とされる電話ＭＴ’（図２）として、隣接の基地局ＢＳ２にログオンし、傍受した呼を単に転送する。

【００１５】装置ＩＣなどによる盗聴に対する機密保護を改善するために、移動電話ＭＴに、例えば図３に示す流れ図にしたがって実行されるハードウェアまたはソフトウェアモジュールを組入れている。

【００１６】移動局ＭＴと基地局の間で無線リンクが確立したら（ステップ１）、伝搬遅延、あるいはこの基地局が移動電話ＭＴに割り当てた送信電力などのこの基地局の特性データが、移動電話ＭＴによって確定される（ステップ２）。それらの新たに確定されたデータは、その移動電話ＭＴ内で、その移動電話ＭＴ内に記憶されているこの基地局への以前の接続時に確定されたデータと比較される（ステップ３）、その比較結果が、その新たに確定されたデータが許容範囲内にあることを示す場合には、それらのデータは移動電話ＭＴ内に記憶され（ステップ４）、その移動局ＭＴと基地局の間の接続の確立は継続する（ステップ５）。ステップ３で使用された許容範囲は、例えば前もってセットしておくかあるいは統計関数を用いて決定してもよい。

【００１７】しかし、新たに確定されたデータと記憶してあるデータとの間に著しい差異がステップ３で検知された場合には、エラー信号が発せられ、プログラムはステップ６に分岐し、そこでその移動電話ＭＴが自身の地上位置を絶対的にまたは基地局に対して相対的に確定する。その地上位置は、データ間の確定された差異と共に、この基地局を介してセンターへ送信される（ステップ７）。そこで、盗聴装置ＩＣの正確な地上位置を、そのメッセージに基づいて、場合によっては他の移動電話から受信した別のメッセージと共に、確定することができる。次にその移動電話ＭＴは、基地局への接続を解除し（ステップ８）、他の基地局と新たな接続を確立する。ユーザが警告メッセージを受信してその接続を解除するか維持するかを決めることもできる。

【００１８】図１および図２の実施形態では、移動電話ＭＴと基地局ＢＳ２の間の伝搬遅延は、介在する盗聴装置ＩＣを介して、無線リンクＦＩＣａとＦＩＣｂとの統合によって、著しく増大する。したがって、比較の結果、盗聴装置（ＩＣ）が不在であった前接続時に確定された伝搬遅延の方が短い場合には、それは著しい差異を示しているので接続が解除される。

【００１９】変形形態では、前記方法を実行するプログラムを記憶媒体内に記憶し、次にその記憶媒体を移動電話の供給者またはユーザに供給し、その供給者またはユ

ーザが移動電話内にプログラムをインストールすることができるようにする。

【００２０】他の変形形態では、プログラムを移動電話にインストールすることができるように、インターネットまたは他のネットワークを介して送信することができる。

【図面の簡単な説明】

【図１】いくつかの基地局、移動電話、および盗聴装置を有する移動無線ネットワークをかなり概略的に示す図である。

【図２】図１の盗聴装置の内部構造をかなり概略的に示す図である。

【図３】盗聴装置を探知し、その地上位置を移動電話を用いて決定するプログラムモジュールに従って実行される方法の例示的な流れ図である。

【符号の説明】

ＢＳ１、ＢＳ２、ＢＳ５　基地局
ＢＳ'　基地局とされる局
ＦＩＣａ、ＦＩＣｂ　リンク
Ｆ２　無線リンク
ＩＣ　盗聴装置
ＭＴ　移動電話
ＭＴ'　移動電話とされる電話
ＲＥＣ　設備

【図１】

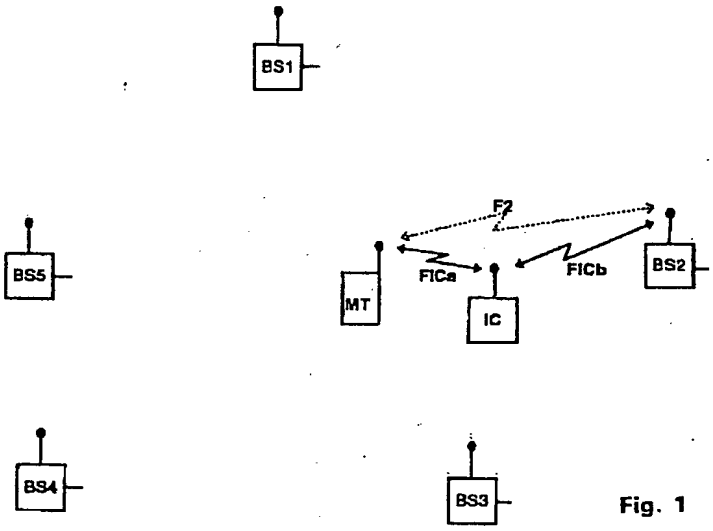


Fig. 1

【図２】

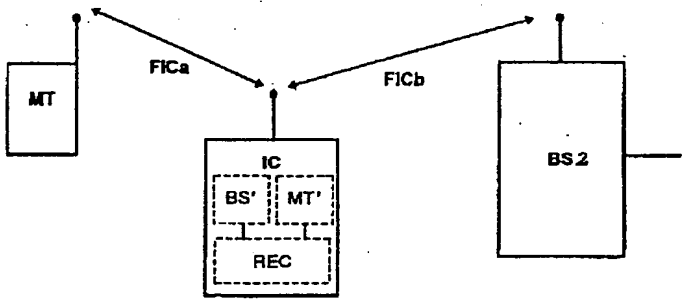


Fig. 2

【図3】

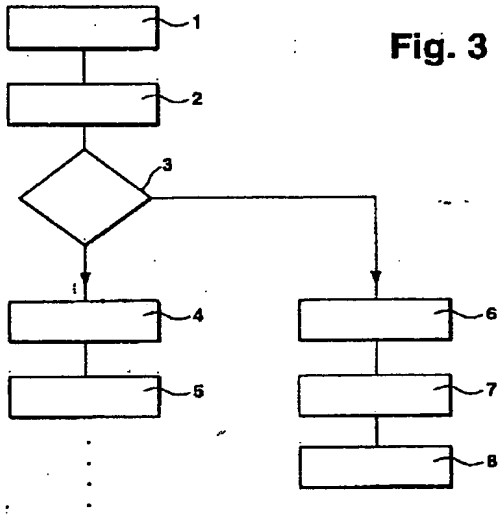


Fig. 3

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード（参考）
		H04L 9/00	691

【外国語明細書】

1. Title of Invention

Improving the Security of Mobile Telephones against Eavesdropping

2. Claims

1. A method of detecting an eavesdropping device (IC) which is interposed between a mobile telephone (MT) and a base station (BS2) and which accepts, as a purported base station (BS'), a call from the mobile telephone (MT) and then forwards it, as a purported mobile telephone (MT'), to the base station (BS2), characterized in that data of the base stations (BS1, ..., BS5) used by the mobile telephone (MT) are stored in the mobile telephone (MT), that when a new connection is set up to a base station (BS2), the data newly determined during this connection setup are compared with the data to be expected for said base station (BS2) in view of the stored data, and that if the data differ, an error signal is generated in the mobile telephone (MT).

2. A method as claimed in claim 1, characterized in that the error signal initiates the release of the connection to said base station (BS2).

3. A method as claimed in claim 1, characterized in that the error signal triggers an alarm message to the user.

4. A method as claimed in claim 1, characterized in that as the data, propagation delays, and/or the transmitting power assigned by the base station (BS2) to the mobile telephone (MT), and/or the mode of encryption specified by the base station (BS2) are used.

5. A method as claimed in claim 1, characterized in that the data include the identities of radio cells and/or of the base stations.

6. A method as claimed in claim 1, characterized in that the data are stored in dependence upon the distance between the mobile telephone (MT) and the base station (BS2).

7. A method as claimed in claim 6, characterized in that the data are stored in groups each relating to at least three base stations separated by a distance from each other.

8. A method as claimed in claim 1, characterized in that the mobile telephone (MT) communicates a determined difference between the data together with information about its geographical position to a center.

9. A computer-readable storage medium having a program recorded thereon, the program carrying out the method claimed in any one of the proceeding claims.

10. A mobile telephone (MT) comprising processor-controlled circuits for carrying out the method as claimed in any one of claims 1 to 8 or comprising a computer-readable storage medium as claimed in claim 9.

3. Detailed Description of Invention

This invention relates to a method of detecting an eavesdropping device which is interposed between a mobile telephone and a base station and which accepts, as a purported base station, a call from the mobile telephone and then forwards it, as a purported mobile telephone, to the base station, as well as to a program module for carrying out this method and to a mobile telephone equipped with such a program module.

Telephoning with digital mobile telephones as are known from the GSM (Global System for Mobile Communications) is considered secure against eavesdropping, since all radio communications between a mobile telephone and a base station are encrypted. In an article entitled "Handys abhörsicher?", published in the journal c't 1998, No. 5, page 92, and in an article entitled "Aus der Luft gegriffen", published in the journal FOCUS, 38/1997, pages 220/221, eavesdropping devices, so-called IMSI catchers (IMSI = International Mobile Subscriber Identity) are described with which mobile telephone calls can possibly be intercepted after all.

These eavesdropping devices act vis-à-vis a mobile telephone like a base station of the mobile radio network. If the eavesdropping device is the strongest transmitter in the vicinity, the mobile telephone will use it as a base station during the next outgoing call. Since, during call establishment, each base station can determine how the radio communication will be encrypted, the eavesdropping device will choose the unencrypted mode. As the eavesdropping device is no genuine base station, it will log on to an adjacent base station as a purported mobile telephone and simply forward the intercepted call as if the latter originated from a mobile telephone.

From EP 0 822 726 A2 it is known to improve security in a radiocommunications network by storing the propagation delay between a fixed telephone and its serving base station at the base station. If the propagation delay measured during another call attempt differs from the stored propagation delay, the telephone will be denied access to the base station.

It is the object of the invention to provide a method of detecting the interposition of the above-described eavesdropping device, a program module for carrying out the method, and a mobile telephone equipped with such a program module.

To attain this object, the invention provides a method of the kind referred to at the beginning which is characterized in that characteristic data of the base stations used by the mobile telephone are stored in the mobile telephone, that when a new connection is set up to a base station, the data newly determined during

this connection setup are compared with the data to be expected for said base station in view of the stored data, and that if the data differ, an error signal is generated in the mobile telephone.

If the newly determined data differ markedly from the stored data as is the case for an interposed eavesdropping device, this error signal may trigger a visual, audible, or mechanical alarm message from the mobile telephone to the user, or the mobile telephone will change to another base station. This measure improves the security of, e.g., GSM mobile stations against eavesdropping. The alarm message can also be transmitted to a center, e.g. for further investigations, possibly using further alarm messages from other mobile subscribers to determine the exact geographical position of the eavesdropping device.

The characteristic data are preferably the propagation delays or the transmitting power assigned by the base station to the mobile telephone. Also, an unencrypted mode desired by the base station can be used as a trigger for the error signal. Further characteristic data could be, for example, the identity of the radio cells or base stations, the response times to enquiries, the geographical distance to the base station, and statistics about the calls conducted with the mobile telephone.

Preferably, these characteristic data are stored in dependence upon the distance between the mobile telephone and the base station so as to be able to interpolate characteristic data for intermediate distances.

If the characteristic data are stored in groups each relating to at least three base stations separated by a distance from each other, interdependent data, such as the propagation delays to the respective base station, can be obtained.

If the mobile telephone communicates a determined difference between the data together with information about its geographical position via the base station to a center, the latter, possibly using further messages received from other mobile telephones, can determine the exact geographical position of the eavesdropping device.

According to a further aspect, the invention also relates to hardware and software modules for carrying out the method described.

Further advantages of the invention are apparent from the following description and the accompanying drawings. According to the invention, the aforementioned features and the features described below can be used alone or in arbitrary combinations. While particular embodiments of the invention are described, it is to be understood that the description is made only by way of example and not as a limitation to the scope of the invention.

Fig. 1 shows a mobile radio network with several base stations BS1 to BS5 and an eavesdropping device IC ("IMSI catcher"). This eavesdropping device IC acts vis-à-vis a mobile station or mobile telephone MT like a base station of the mobile radio network. In the embodiment shown it is assumed that the mobile telephone MT would have selected the base station BS2 as the strongest station for the establishment of a call over the radio link F2 if the eavesdropping device IC were not present or not active. Since the eavesdropping device IC is the strongest transmitter in the vicinity of the mobile telephone MT, however, the mobile telephone MT will use it as a supposed base station BS' (Fig. 2) during the next outgoing call. Accordingly, the link FICa to the eavesdropping device IC is established. Since during a connection setup each base station can determine how the radio communication will be encrypted, the eavesdropping device IC will select the unencrypted mode. Via a facility REC provided in the eavesdropping device IC, the conversation can then be listened to or recorded. Via the link FICb, the eavesdropping device IC will log, as a purported mobile telephone MT' (Fig. 2), on to the

adjacent base station BS2 and simply forward the intercepted call.

To improve the security against eavesdropping by means of such a device IC, the mobile telephone MT incorporates a hardware or software module that operates, for example, according to the flowchart shown in Fig. 3.

After a radio link has been established between the mobile station MT and a base station (step 1), characteristic data of this base station, such as propagation delays or the transmitter power assigned by this base station to the mobile telephone MT, are determined by the mobile telephone MT (step 2). These newly determined data are compared (step 3) in the mobile telephone MT with the data determined during previous connections with this base station, which were stored in the mobile telephone MT. If this comparison indicates that the newly determined data lie within permissible limits, these data will be stored in the mobile telephone MT (step 4) and the setting up of the connection between the mobile station MT and the base station will continue (step 5). The permissible limits used in step 3 may be preset or be determined using statistical functions, for example.

If, however, a significant difference between the newly determined data and the stored data is detected in step 3, an error signal will be generated and the program will branch to step 6, in which the mobile telephone MT determines its geographical position, absolutely or relative to the base station. This geographical position, together with the determined difference

between the data, is communicated via this base station to a center (step 7). There, the exact geographical position of the eavesdropping device IC can be determined based on this message, possibly together with further messages received from other mobile telephones. The mobile telephone MT will then release the connection with the base station (step 8) and establish a new connection to another base station. It is also possible for the user to receive an alarm message and then decide whether to release or maintain the connection.

In the embodiments of Figs. 1 and 2, the propagation delays between mobile telephone MT and base station BS2 are significantly increased by the combined radio link FICa and FICb via the interposed eavesdropping device IC. Therefore, the comparison with the shorter propagation delays determined during previous connections without an interposed eavesdropping device IC will indicate a marked difference, so that the connection will be released.

In a variant, a program carrying out the method described above may be stored in a storage medium and then the storage medium is delivered to the supplier or the user of mobile phones so that the supplier or the user can install the program in mobile phones.

In another variant, the program can be transmitted through the Internet or other networks so that it can be installed in mobile phones.

4. Brief Description of Drawings

Fig. 1 shows highly schematically a mobile radio network with several base stations, a mobile telephone, and an eavesdropping device.

Fig. 2 shows highly schematically the internal structure of the eavesdropping device of Fig. 1.

Fig. 3 is an exemplary flowchart for a method carried out in accordance with a program module to detect the eavesdropping device and determine its geographical position using the mobile telephone.

Fig. 1

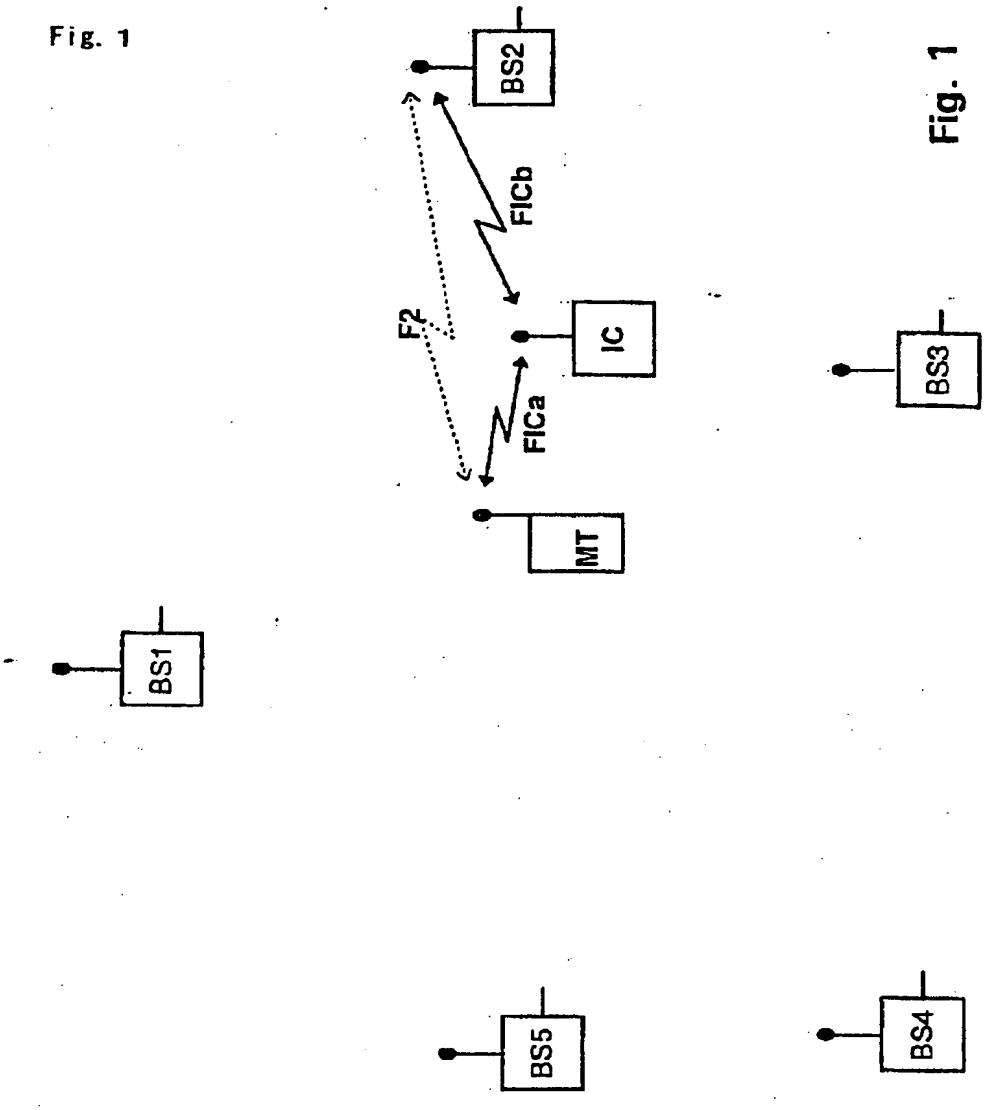


Fig. 1

Fig. 2

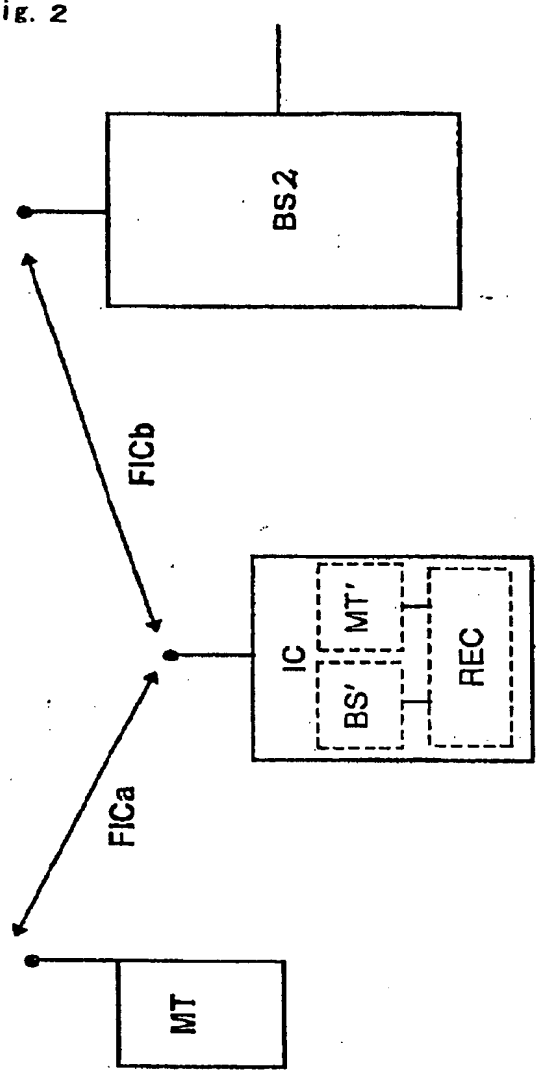
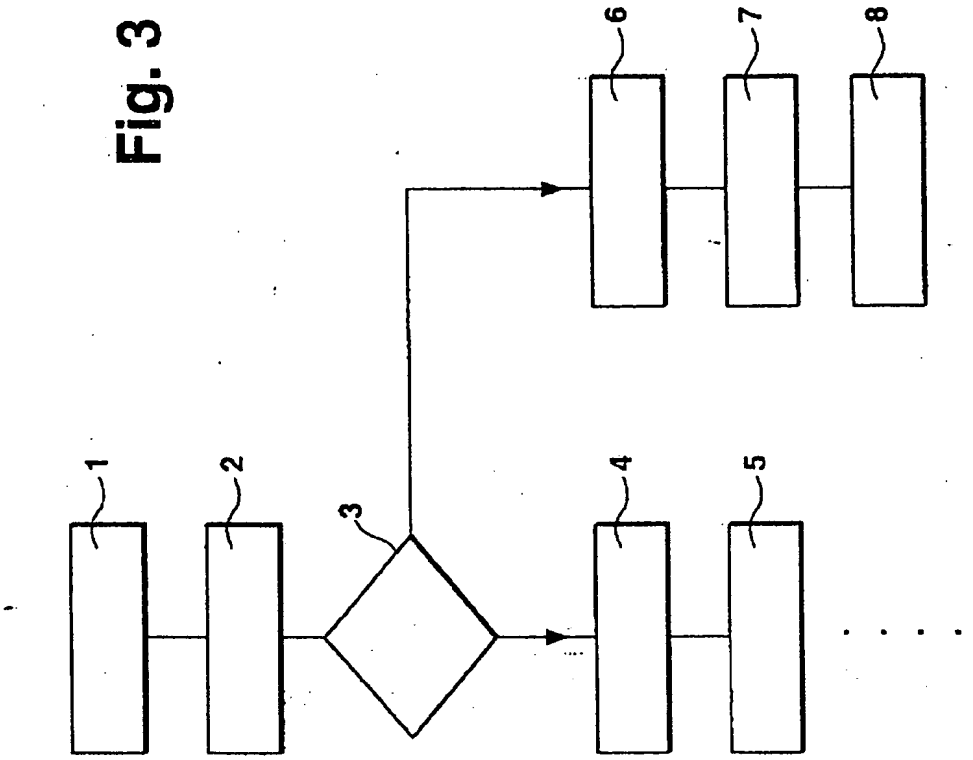


Fig. 2

Fig. 3



1. Abstract

A method of detecting an eavesdropping device (IC) which is interposed between a mobile telephone (MT) and a base station (BS2) and which accepts, as a purported base station, a call from the mobile telephone (MT) and then forwards it, as a purported mobile telephone, to the base station (BS2) involves storing data of the base stations (BS1, ..., BS5) used by the mobile telephone (MT) in the mobile telephone (MT). When a new connection is set up to a base station (BS2), the data newly determined during this connection setup are compared with the data to be expected for this base station (BS2) in view of the stored data. If the data differ, an error signal is generated in the mobile telephone (MT). This error signal may initiate a release of the connection with this base station (BS2) or trigger an alarm message to the user. This improves the security of, e.g., GSM mobile stations against eavesdropping.

2. Representative Drawing

Fig. 1